



Azure Fundamentals Workshop

24. Februar 2020
Version 1.0

Autor

ACP IT Solutions GmbH
Johannes Lagler-Gruener
+43 1 89193 11809
johannes.lagler-gruener@acp.at



Contents

Demo Hand-Out für User tn2:	3
Solution Übersicht:	3
Schritt für Schritt Anleitung	4
Einrichten der Netzwerk Umgebung	4
Einrichten der virtuellen Netzwerke	4
Einrichten der Azure Network Security Groups	5
Anpassen der Network Security Groups	6
Binden der Network Security Groups	8
VNet Peering erstellen	8
Einrichten der Frontend Infrastruktur	9
VM in West Europe	9
VM in EastUS2	10
Azure Automation DSC Configuration binden	11
(Optional) Powershell Configuration enforce	13
Azure Traffic Manager einrichten	15
DNS Label auf PIP setzen	15
Azure Traffic Manager Profile konfigurieren	16
Azure Backup einrichten (Variante1) für West Europe	17
Azure Backup einrichten (Variante2) für EastUS2	18
Azure Monitoring einrichten	19
Fertige Solution überprüfen	20
Überprüfen der Applikation	20
Überprüfen der Traffic Manager Funktionalität	20
Überprüfen des VM Backups	21
Überprüfen des VM Monitorings	21



Demo Hand-Out für User tn2:

URL: <https://portal.azure.com>

Login: tn2@demo.acp.at

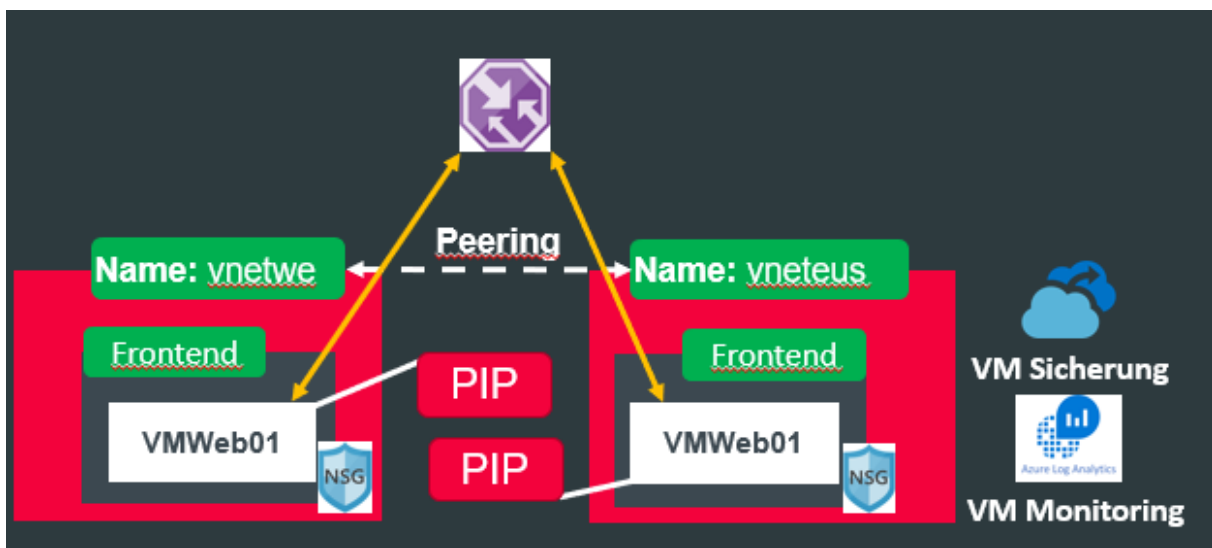
Shortname: tn2

Passwort: AzFundamentalsWs01

Muss bei der ersten Anmeldung geändert werden!

Ressource Gruppe: AFW-tn2-demo1

Solution Übersicht:





Schritt für Schritt Anleitung.

- Öffnen des Azure Portals <https://portal.azure.com>.
- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)

Einrichten der Netzwerk Umgebung.

Einrichten der virtuellen Netzwerke

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
 - In den Azure Marketplace wechseln „Add“ und die Ressource „Virtual Network“ suchen und auf „Create“ klicken.
 - Die folgenden Parameter eingeben:
 - **Name:** vnetwe
 - **Address space:** 10.1.0.0/16
 - **Subscription:** AZURE CSP....
 - **ResourceGroup:** AFW-tn2-demo1
 - **Location:** WestEurope
 - **Subnet:** Frontend
 - **Address Range:** 10.1.0.0/24
 - **DDos:** Basic
 - **Service Endpoint:** Disabled
 - **Firewall:** Disabled
 - Anschließend auf „Create“ klicken.
-
- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
 - In den Azure Marketplace wechseln „Add“ und die Ressource „Virtual Network“ suchen und auf „Create“ klicken.
 - Die folgenden Parameter eingeben:
 - **Name:** vneteus
 - **Address space:** 10.2.0.0/16
 - **Subscription:** AZURE CSP....
 - **ResourceGroup:** AFW-tn2-demo1
 - **Location:** EastUs2
 - **Subnet:** Frontend
 - **Address Range:** 10.2.0.0/24
 - **DDos:** Basic
 - **Service Endpoint:** Disabled
 - **Firewall:** Disabled
 - Anschließend auf „Create“ klicken.



Einrichten der Azure Network Security Groups

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In den Azure Marketplace wechseln „**Add**“ und die Ressource „**Network security group**“ suchen und auf „**Create**“ klicken.
- Die folgenden Parameter eingeben:
 - **Name:** nsgwefrontend
 - **Subscription:** AZURE CSP....
 - **ResourceGroup:** AFW-tn2-demo1
 - **Location:** WestEurope
- Auf „**Create**“ klicken

- Unter ResourceGroups in die für die Demo vorgesehene ResourceGruppe wechseln (AFW-tn2-demo1)
- In den Azure Marketplace wechseln „**Add**“ und die Ressource „**Network security group**“ suchen und auf „**Create**“ klicken.
- Die folgenden Parameter eingeben:
 - **Name:** nsgeusfrontend
 - **Subscription:** AZURE CSP....
 - **ResourceGroup:** AFW-tn2-demo1
 - **Location:** EastUs2
- Auf „**Create**“ klicken



Anpassen der Network Security Groups

- In der ResourceGroup „**AFW-tn2-demo1**“ die Network Security Group „**nsgwefrontend**“ auswählen und unter „**Inbound security rules**“ mit dem Button „**Add**“ die folgenden Rules einfügen:
- Port80 Rule
 - **Source:** Any
 - **Source Port Range:** *
 - **Destination:** Any
 - **Destination Port Range:** 80
 - **Protocol:** TCP
 - **Action:** Allow
 - **Priority:** 100
 - **Name:** Allow_Port80
- Auf „**Add**“ klicken

- In der ResourceGroup „**AFW-tn2-demo1**“ die Network Security Group „**nsgwefrontend**“ auswählen und unter „**Inbound security rules**“ mit dem Button „**Add**“ die folgenden Rules einfügen:
- Port3389 Rule
 - **Source:** Ip Addresses von ihrem Host (in Google nach „**my IP**“ suchen)
 - **Source Port Range:** *
 - **Destination:** Any
 - **Destination Port Range:** 3389
 - **Protocol:** Any
 - **Action:** Allow
 - **Priority:** 101
 - **Name:** Allow_Port3389
- Auf „**Add**“ klicken



- In der ResourceGroup „**AFW-tn2-demo1**“ die Network Security Group „**nsgeusfrontend**“ auswählen und unter „**Inbound security rules**“ mit dem Button „**Add**“ die folgenden Rules einfügen:
- Port80 Rule
 - **Source:** Any
 - **Source Port Range:** *
 - **Destination:** Any
 - **Destination Port Range:** 80
 - **Protocol:** TCP
 - **Action:** Allow
 - **Priority:** 100
 - **Name:** Allow_Port80
- Auf „**Add**“ klicken

- In der ResourceGroup „**AFW-tn2-demo1**“ die Network Security Group „**nsgeusfrontend**“ auswählen und unter „**Inbound security rules**“ mit dem Button „**Add**“ die folgenden Rules einfügen:
- Port3389 Rule
 - **Source:** Ip Addresses von ihrem Host (in Google nach „**my IP**“ suchen)
 - **Source Port Range:** *
 - **Destination:** Any
 - **Destination Port Range:** 3389
 - **Protocol:** Any
 - **Action:** Allow
 - **Priority:** 101
 - **Name:** Allow_Port3389
- Auf „**Add**“ klicken



Binden der Network Security Groups

- In der ResourceGroup „**AFW-tn2-demo1**“ das virtuelle Netzwerk „**vnetwe**“ auswählen und unter Subnets das „**frontend**“ Subnet auswählen.
- Im Bereich „**Network security group**“ die Network Security Group „**nsgwefrontend**“ auswählen und auf „**speichern**“ klicken.
- In der ResourceGroup „**AFW-tn2-demo1**“ das virtuelle Netzwerk „**vneteus**“ auswählen und unter Subnets das „**frontend**“ Subnet auswählen.
- Im Bereich „**Network security group**“ die Network Security Group „**nsgeusfrontend**“ auswählen und auf „**speichern**“ klicken.

VNet Peering erstellen

- In der ResourceGroup „**AFW-tn2-demo1**“ das virtuelle Netzwerk „**vnetwe**“ in den Bereich „**Peerings**“ wechseln.
- Den Button „**Add**“ auswählen und die folgenden Parameter eingeben:
 - **Name:** p-we-to-eus
 - **Virtual network deployment model:** Resource manager
 - **I know my resource ID:** nicht auswählen
 - **Subscription:** AZURE CSP...
 - **Virtual Network:** vneteus
 - **Name of the peering from vneteus to vnetwe:** p-eus-to-we
 - Restliche Einstellungen belassen.



Einrichten der Frontend Infrastruktur

VM in West Europe

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In den Azure Marketplace wechseln „**Add**“ und die Ressource „**Windows Server**“ suchen, die Version „**[smalldisk] Windows Server 2016 Datacenter**“ auswählen und auf „**Create**“ klicken.
- Die folgenden Einstellungen in der „**Basic**“ View treffen:
 - **Subscription:** AZURE CSP...
 - **Resource Group:** AFW-tn2-demo1
 - **Virtual Machine Name:** afw-tn2-we-d1
 - **Region:** West Europe
 - **Availability options:** No infrastructure redundancy required
 - **Image:** [smalldisk] Windows Server 2016 Datacenter
 - **Size:** Standard DS2 v2
 - **Username:** adminuser
 - **Passwort:** AzFundamentalsWs01
 - **Public inbound ports:** None
 - **Already have a Windows Server license:** No
- Auf „**Next: Disk >**“ klicken.
- Die folgenden Einstellungen in der „**Disk**“ View treffen:
 - **OS disk type:** Standard SSD
- Auf „**Next: Networking >**“ klicken
- Die folgenden Einstellungen in der „**Networking**“ View treffen:
 - **Virtual network:** vnetwe
 - **Subnet:** Frontend
 - **Public IP:** Einstellungen belassen
 - **Nic network security group:** None
 - **Accelerated networking:** On
 - **Load Balancing:** No
- Auf „**Next: Management >**“ klicken
- Die Einstellungen so belassen und auf „**Next: Advanced >**“ klicken
- Die Einstellungen so belassen und auf „**Next: Tags >**“ klicken
- Die Einstellungen so belassen und auf „**Next: Review + create >**“ klicken
- Sofern die Validierung erfolgreich war auf „**create**“ klicken.



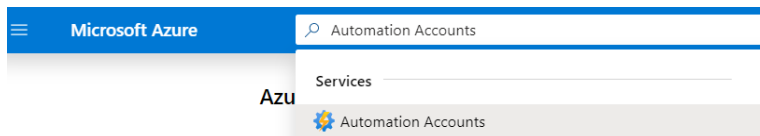
VM in EastUS2

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In den Azure Marketplace wechseln „Add“ und die Ressource „**Windows Server**“ suchen, die Version „[smalldisk] **Windows Server 2016 Datacenter**“ auswählen und auf „**Create**“ klicken.
- Die folgenden Einstellungen in der „**Basic**“ View treffen:
 - **Subscription:** AZURE CSP...
 - **Resource Group:** AFW-tn2-demo1
 - **Virtual Machine Name:** afw-tn2-eus-d1
 - **Region:** EastUS2
 - **Availability options:** No infrastructure redundancy required
 - **Image:** [smalldisk] Windows Server 2016 Datacenter
 - **Size:** Standard DS2 v2
 - **Username:** adminuser
 - **Passwort:** AzFundamentalsWs01
 - **Public inbound ports:** None
 - **Already have a Windows Server license:** No
- Auf „**Next: Disk** >“ klicken.
- Die folgenden Einstellungen in der „**Disk**“ View treffen:
 - **OS disk type:** Standard SSD
- Auf „**Next: Networking** >“ klicken
- Die folgenden Einstellungen in der „**Networking**“ View treffen:
 - **Virtual network:** vneteus
 - **Subnet:** Frontend
 - **Public IP:** Einstellungen belassen
 - **Nic network security group:** None
 - **Accelerated networking:** On
 - **Load Balancing:** No
- Auf „**Next: Management** >“ klicken
- Die Einstellungen so belassen und auf „**Next: Advanced** >“ klicken
- Die Einstellungen so belassen und auf „**Next: Tags** >“ klicken
- Die Einstellungen so belassen und auf „**Next: Review + create** >“ klicken
- Sofern die Validierung erfolgreich war auf „**create**“ klicken.

Azure Automation DSC Configuration binden

!WICHTIG! Die Provisionierung der virtuellen Maschinen muss abgeschlossen sein, um diese Schritte durchzuführen!

Im oberen Bereich in der Suche „Automation Accounts“ eingeben und anschließend das Service auswählen.



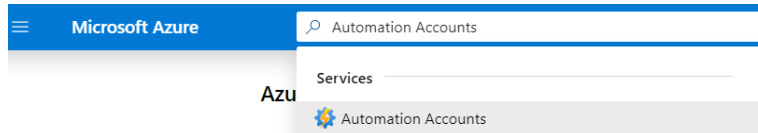
- Den Automation Account „ACP-Demo-Level1-WS“ auswählen und in den Bereich „**State configuration (DSC)**“ wechseln.
- Im oberen Bereich des Automation Accounts auf „**+ Add**“ klicken.

Task1: Die Virtuelle Maschine in EUS in DSC binden

- Die Virtuelle Maschine „**afw-tn2-eus-d1**“ auswählen.
- Anschließend auf „**+ Connect**“ klicken und die folgenden Einstellungen treffen:
 - **Registration key:** Primary key
 - **Node configuration name:** dsceus.WebServerConfig
 - **Refresh Frequency:** 30
 - **Configuration Mode Frequency:** 15
 - **Configuration Mode:** ApplyAndAutoCorrect
 - **Allow Module Override:** auswählen
 - **Reboot if Needed:** auswählen
 - **Action after Reboot:** ContinueConfiguration
- Auf „**OK**“ klicken (Dieser Task kann bis zu 15 Minuten dauern)



Im oberen Bereich in der Suche „Automation Accounts“ eingeben und anschließend das Service auswählen.



- Den Automation Account „ACP-Demo-Level1-WS“ auswählen und in den Bereich „**State configuration (DSC)**“ wechseln.
- Im oberen Bereich des Automation Accounts auf „**+ Add**“ klicken.

Task2: Die Virtuelle Maschine in WE in DSC binden

- Die Virtuelle Maschine „**afw-tn2-we-d1**“ auswählen.
- Anschließend auf „**+ Connect**“ klicken und die folgenden Einstellungen treffen:
 - **Registration key:** Primary key
 - **Node configuration name:** dscwe.WebServerConfig
 - **Refresh Frequency:** 30
 - **Configuration Mode Frequency:** 15
 - **Configuration Mode:** ApplyAndAutoCorrect
 - **Allow Module Override:** auswählen
 - **Reboot if Needed:** auswählen
 - **Action after Reboot:** ContinueConfiguration
- Auf „**OK**“ klicken (Dieser Task kann bis zu 15 Minuten dauern)



(Optional) Powershell Configuration enforce

Diese Option ist ein optionaler Schritt. Normalerweise würde die Umsetzung der Konfiguration bis zu 30 Minuten dauern. Um die Konfiguration manuell zu starten gibt es zwei Varianten:

- Via RDP auf die VM verbinden und die Konfiguration mittels Powershell Befehl anstoßen.
- Via Azure Serial Console auf die VM verbinden, die Powershell öffnen und mittels Powershell Befehl die Configuration anstoßen.

In diesem Schritt beschreibe ich die Variante 2, da dies auch im Falle der Fehlerbehebung einer VM hilfreich sein könnte.

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In der Ressource Gruppe die Virtual Machine Object „**afw-tn2-we-d1**“ öffnen und in den Bereich „**Serial console**“ wechseln.
- In der Commandline den Befehlen „**cmd**“ eingeben und auf „**enter**“ klicken
- In der Commandline den Befehl „**ch**“ eingeben und auf „**enter**“ klicken
- In der Commandline wird jetzt der Channel ausgegeben, auf welchen eine Verbindung aufgebaut werden kann. Bitte die Nummer herausuchen für den Channel „**CMD00X**“
- In der Commandline den Befehl „**ch -si X**“ X steht für die Channel Nummer eingeben und „**enter**“ klicken.
- Anschließend nochmals „**enter**“ klicken, um zu bestätigen
- Jetzt kommt die Aufforderung für den Login. Bitte Folgendes eintragen:
 - **Username:** adminuser
 - **Domain:**
 - **Passwort:** AzFundamentalsWs01
- Sobald das cmd window gestartet hat, bitte den Befehl „**Powershell**“ eingeben.
- Den folgenden Befehl eingeben: „**Update-DscConfiguration -Wait -Verbose -Debug**“
- Auf „**enter**“ klicken
- Den folgenden Befehl eingeben: „**Start-DscConfiguration –UseExisting –Verbose –Wait**“
- Auf „**enter**“ klicken
- In die Commandline den Befehl „**exit**“ eingeben und auf „**enter**“ klicken.
- In die Commandline den Befehl „**exit**“ eingeben und auf „**enter**“ klicken.

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In der Ressource Gruppe die Virtual Machine Object „**afw-tn2-eus-d1**“ öffnen und in den Bereich „**Serial console**“ wechseln.
- In der Commandline den Befehlen „**cmd**“ eingeben und auf „**enter**“ klicken
- In der Commandline den Befehl „**ch**“ eingeben und auf „**enter**“ klicken
- In der Commandline wird jetzt der Channel ausgegeben, auf welchen eine Verbindung aufgebaut werden kann. Bitte die Nummer herausuchen für den Channel „**CMD00X**“
- In der Commandline den Befehl „**ch -si X**“ X steht für die Channel Nummer eingeben und „**enter**“ klicken.
- Anschließend nochmals „**enter**“ klicken, um zu bestätigen
- Jetzt kommt die Aufforderung für den Login. Bitte Folgendes eintragen:
 - **Username:** adminuser
 - **Domain:**
 - **Passwort:** AzFundamentalsWs01
- Sobald das cmd window gestartet hat, bitte den Befehl „**Powershell**“ eingeben.
- Den folgenden Befehl eingeben: „**Update-DscConfiguration -Wait -Verbose -Debug**“
- Auf „**enter**“ klicken
- Den folgenden Befehl eingeben: „**Start-DscConfiguration -UseExisting -Verbose -Wait**“
- Auf „**enter**“ klicken
- In die Commandline den Befehl „**exit**“ eingeben und auf „**enter**“ klicken.
- In die Commandline den Befehl „**exit**“ eingeben und auf „**enter**“ klicken.



Azure Traffic Manager einrichten

DNS Label auf PIP setzen

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In der Ressource Gruppe die Public IP „**afw-tn2-eus-d1-ip**“ öffnen und in den Bereich „**Configuration**“ wechseln.
- Im Bereich „**DNS name label (optional)**“ „**afwtneusd1tn2dns**“ eintragen
- Auf „**Save**“ klicken.

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In der RessourceGruppe die Public IP „**afw-tn2-we-d1-ip**“ öffnen und in den Bereich „**Configuration**“ wechseln.
- Im Bereich „**DNS name label (optional)**“ „**afwtnwed1tn2dns**“ eintragen
- Auf „**Save**“ klicken.



Azure Traffic Manager Profile konfigurieren

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In den Azure Marketplace wechseln „Add“ und die Ressource „Traffic Manager profile“ und auf „Create“ klicken.
- Die folgenden Einstellungen treffen
 - **Name:** afw-tn2-demo1-trm
 - **Routing Methode:** Performance
 - **Subscription:** AZURE CSP....
 - **ResourceGroup:** afw-tn2-demo1
- Auf „create“ klicken.
- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In der Ressource Gruppe in das Traffic Manager Profil „afw-tn2-demo1-trm“ öffnen und in den Bereich „Endpoints“ wechseln.
- Dort die folgenden Einstellungen treffen:
 - „Add“ klicken.
 - **Type:** Azure endpoint
 - **Name:** AzEPWE
 - **Target resource type:** Public IP address
 - Target resource auswählen
 - „afw-tn2-we-d1-ip“ auswählen
 - **Custom Header settings:** belassen
 - **Add as disabled:** nicht aktivieren
 - Auf „OK“ klicken
 - „Add“ klicken.
 - **Type:** Azure endpoint
 - **Name:** AzEPEUS
 - **Target resource type:** Public IP address
 - Target resource auswählen
 - „afw-tn2-eus-d1-ip“ auswählen
 - **Custom Header settings:** belassen
 - **Add as disabled:** nicht aktivieren
 - Auf „OK“ klicken

Azure Backup einrichten (Variante1) für West Europe

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (**AFW-tn2-demo1**)
- In den Azure Marketplace wechseln „**Add**“ und die Ressource „**Backup and Site Recovery**“ und auf „**Create**“ klicken.
- Die folgenden Einstellungen treffen
 - **Subscription:** AZURE CSP....
 - **ResourceGroup:** afw-tn2-demo1
 - **Vault Name:** afw-tn2-we-backup
 - **Region:** West Europe
- Auf „**Review + create**“ klicken.
- Auf „**create**“ klicken.
- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (**AFW-tn2-demo1**)
- In der Ressource Gruppe das Recovery Services Vault Service „**afw-tn2-we-backup**“ öffnen und in den Bereich „**Properties**“ wechseln.
- Dort die folgenden Einstellungen treffen:
 - Security Settings (Update)
 - Soft Delete (For Azure Virtual Machines): Disable

Have you configured [Azure Multi-Factor Authentication](#)?

Soft Delete

(For Azure Virtual Machines)

* Soft delete feature cannot be disabled if you have protected item(s) in the vault

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (**AFW-tn2-demo1**)
- In der Ressource Gruppe das Recovery Services vault Service „**afw-tn2-we-backup**“ öffnen und in den Bereich „**Backup**“ wechseln.
- Die folgende Auswahl treffen:
 - Where is your workload running?: Azure
 - What do you want to backup?: Virtual machine
 - Klick **Backup**
- Bei Backup Backup policy folgende Auswahl treffen:
 - Choose backup policy: Create new
 - **Policy name:** afw-tn2-we-policy
 - **Frequency:**
 - Daily
 - 01:00 AM
 - UTC + (01:00) Amsterdam, Berlin,...
- Auf **OK** klicken
- Die zuvor angelegte Virtuelle Maschine „afw-tn2-we-d1“ auswählen und auf „**OK**“ klicken.
- Anschließend auf „**Enable backup**“ klicken.



Azure Backup einrichten (Variante2) für EastUS2

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (**AFW-tn2-demo1**)
- In den Azure Marketplace wechseln „Add“ und die Ressource „Backup and Site Recovery“ und auf „Create“ klicken.
- Die folgenden Einstellungen treffen
 - **Subscription:** AZURE CSP....
 - **ResourceGroup:** afw-tn2-demo1
 - **Vault Name:** afw-tn2-eus-backup
 - **Region:** EastUS2
- Auf **“Review + create”** klicken.
- Auf **“create”** klicken.
- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (**AFW-tn2-demo1**)
- In der Ressource Gruppe das Recovery Services vault Service „afw-tn2-eus-backup“ öffnen und in den Bereich **„Properties“** wechseln.
- Dort die folgenden Einstellungen treffen:
 - Security Settings (Update)
 - Soft Delete (For Azure Virtual Machines): Disable

Have you configured [Azure Multi-Factor Authentication](#)?

Soft Delete

(For Azure Virtual Machines)

Enable

Disabled

* Soft delete feature cannot be disabled if you have protected item(s) in the vault

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (**AFW-tn2-demo1**)
- In der Ressource Gruppe die Virtual Machine Object „afw-tn2-eus-d1“ öffnen und in den Bereich **„Backup“** wechseln.
- Die folgende Auswahl treffen:
 - Select existing
 - **Name:** afw-tn2-eus-backup
 - **Choose backup policy:** Create (or edit) a new policy
 - **Policy name:** afw-tn2-eus-policy
 - **Frequency:**
 - Daily
 - 01:00 AM
 - UTC + (01:00) Amsterdam, Berlin,...
- Auf **“OK”** klicken.
- Auf **“Enable Backup”** klicken.



Azure Monitoring einrichten

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
 - In den Azure Marketplace wechseln „**Add**“ und die Ressource „**Log Analytics**“ suchen und auf „**Create**“ klicken.
 - Die Folgende Auswahl treffen:
 - **Log Analytics Workspace:** afw-tn2-we-loga
 - **Subscription:** AZURE CSP...
 - **Resource Group:** AFW-tn2-demo1
 - **Location:** West Europe
 - **Pricing tier:** Per (GB) 2018
 - Auf „**OK**“ klicken.
-
- In der Ressource Gruppe das Virtual Machine Object „**afw-tn2-eus-d1**“ öffnen und in den Bereich „**Insights (preview)**“ wechseln.
 - Die folgende Auswahl treffen:
 - **Workspace Subscription:** AZURE CSP...
 - **Choose a Log Analytics Workspace:** afw-tn2-we-loga
 - Auf „**Enable**“ klicken.
-
- In der Ressource Gruppe das Virtual Machine Object „**afw-tn2-we-d1**“ öffnen und in den Bereich „**Insights (preview)**“ wechseln.
 - Die folgende Auswahl treffen:
 - **Workspace Subscription:** AZURE CSP...
 - **Choose a Log Analytics Workspace:** afw-tn2-we-loga
 - Auf „**Enable**“ klicken.



Fertige Solution überprüfen

Die Solution sollte nach Abschluss der oben definierten Schritte fertig implementiert sein. Um dies zu verifizieren sind folgende Schritte notwendig:

Überprüfen der Applikation

Um zu überprüfen, ob die Applikation lauffähig ist, muss im ersten Schritt einmal die URL des Traffic Managers herausgefunden werden.

Hierzu sind die folgenden Schritte notwendig:

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In der Ressource Gruppe das Traffic Manager Object „**afw-tn2-demo1-trm**“ öffnen und in den Bereich „**Overview**“ wechseln.
- Auf der rechten Seite ist der „DNS name“ ersichtlich. Diesen URL kopieren und in einen Browser (in private mode) öffnen
- Die Website mit dem Text „**Yesss, meine Applikation laeuft! Dieser Webserver befindet sich in West Europe**“ sollte erscheinen.
- Den Browser Cache löschen und alle Browser schließen.

Überprüfen der Traffic Manager Funktionalität

- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In der Ressource Gruppe das Traffic Manager Object „**afw-tn2-demo1-trm**“ öffnen und in den Bereich „**Endpoints**“ wechseln.
- Den Endpoint „AzEPWE“ auswählen und anschließend den Punkt „Status“ auf „disabled“ setzen.
- Auf „Save“ klicken
- In der Ressource Gruppe das Traffic Manager Object „**afw-tn2-demo1-trm**“ öffnen und in den Bereich „**Overview**“ wechseln.
- Auf der rechten Seite ist der „DNS name“ ersichtlich. Diesen URL kopieren und in einem Browser (in private mode) öffnen
- Die Website mit dem Content „**Yesss, meine Applikation laeuft! Dieser Webserver befindet sich in EastUS2**“ sollte erscheinen.

Überprüfen des VM Backups

Das Backup an sich, würde erst um 01:00AM laufen, jedoch kann überprüft werden, ob der Backup „Pre Check“ erfolgreich durchgeführt worden ist.

Hierzu sind die folgenden Schritte notwendig:

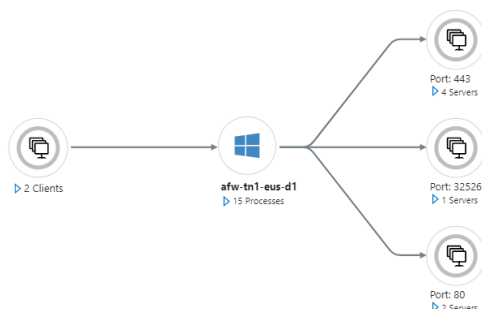
- Unter ResourceGroups in die für die Demo vorgesehene ResourceGruppe wechseln (AFW-tn2-demo1)
- In der RessourceGruppe das Recovery Services Vault object „**afw-tn2-eus-backup**“ öffnen und in den Bereich „**Backup items**“ wechseln.
- Anschließend den Bereich „**Azure Virtual Machine**“ auswählen.
- Im unteren Bereich sollte sich die virtuelle Maschine mit den Namen „**afw-tn2-eus-d1**“ befinden und den „**BACKUP PRE-CHECK**“ „**Passed**“ aufweisen.
- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In der Ressource Gruppe das Recovery Services Vault Object „**afw-tn2-we-backup**“ öffnen und in den Bereich „**Backup items**“ wechseln.
- Anschließend den Bereich „**Azure Virtual Machine**“ auswählen.
- Im unteren Bereich sollte sich die virtuelle Maschine mit dem Namen „**afw-tn2-we-d1**“ befinden und den „**BACKUP PRE-CHECK**“ „**Passed**“ aufweisen.

Überprüfen des VM Monitorings

Durch die oben implementierten Schritte ist ein „Basis“ Monitoring der virtuellen Maschine verfügbar.

Um den Status zu überprüfen sind folgende Schritte notwendig:












- Unter ResourceGroups in die für die Demo vorgesehene Ressource Gruppe wechseln (AFW-tn2-demo1)
- In der Ressource Gruppe das Virtual Maschine Object „**afw-tn2-eus-d1**“ öffnen und in den Bereich „**Insights (preview)**“ wechseln.
- Dort müsste einerseits im Bereich „**Map**“ ein Connection Map verfügbar sein:





- Und zusätzlich im Bereich „**Health**“ unter „**Guest VM health**“ die VM auf ihre Basiskonfiguration gemonitort werden.

Guest VM health

CATEGORY	HEALTH STATUS
 Guest VM health	 Healthy
CPU - _Total	 Healthy
Disk - 0 C:	 Healthy
Disk - 1 D:	 Healthy
LogicalDisk - C:	 Healthy
LogicalDisk - D:	 Healthy
Memory - Memory	 Healthy
NetworkAdapter - Mellanox ConnectX-3 Virtual Fu...	 Healthy
NetworkAdapter - Microsoft Hyper-V Network Ad...	 Healthy
Service - afw-tn1-eus-d1	 Healthy